Affecting Factors in Information Security Policy Compliance: Combine Organisational Factors and User Habits

by Okfalisa Okfalisa

Submission date: 07-Jan-2021 09:03AM (UTC+0700)
Submission ID: 1483921303
File name: Affecting_factors.pdf (229.39K)
Word count: 4366
Character count: 25298

Affecting Factors in Information Security Policy Compliance: Combine Organisational Factors and User Habits

Angraini[1,4], Rose Alinda Alias[2] and Okfalisa[3]

[1]School of Computing, Faculty Engineering, University Technology Malaysia, 81310 Johor, Malaysia
[2]Department of Information System, Azman Hashim International Business School, University Technology Malaysia,81310 Johor Malaysia
[3]Department of Informatics Engineering, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau
[4]Department of Information System, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau
Angraini@uin-suska.ac.id

Abstract. Information security policy compliance is one concern of organisations to improve information security, including universities. Previous research has shown that factors that influence user compliance can come from user behaviour and from within the organisation. This study aims to explore the factors of organisation and user habits that affect user compliance with information security policies. The research model proposed used organisational commitment, organisational culture, reward, and habit variables—this research conducted with a case study of public universities in Indonesia by using an online survey. The results indicated that the factors derived from organisational commitment established a positive influence on the user's respectful behaviour. The insignificant organisational culture and reward affected information security policies. User habits also influenced user behaviour in maintaining information security.

Keywords: compliance, information security policy, organisation commitment, organisation culture, habit.

1 Introduction

There has been a growth in research to devote more attention to information security due to a significant increase in threats and attacks on information security. Cybersecurity Ventures estimates that a business will fall victim to ransomware attacks every 14 seconds in 2019 and every 11 seconds in 2021 [1]. universities are one of targeting information security attacks because they have confidential data.(Symantec,2017, 2018). An increase in the number of security violations experienced in recent years by higher education than the importance of confidentiality, integrity, and availability of information at the university (Bongiovanni 2019).

Information Security protection conducted technically and strategically by using security policies as a guide for their employees to protect user information. The organisation considers system users are considered the most unprotected part of the information security system [2]. Almost 60% of IT managers believe employee negligence to establish an organisation lose millions of dollars as a severe threat to information security [3]. The organisation is aware of the much information security threat that can come from inside or outside the organisation. Therefore, it is essential for organisations always to ensure their information security policies are applied continuously. However, employees are often even unprepared to comply with these procedures and guidelines. Whereas, information system security policies made to secure the company IS assets and prevent misuse of the destruction of its information system [4, 5]. Hence, it is necessary to recognise the factors that influence users to comply with security policies which influence users to adhere to information security policies can originate from organisational or human behaviour. Several researchers have examined to determine the factors that influence users to comply with information security policies. Human and organisational factors represent factors that influence compliance with information security policies [6]

Empirical Data from D'Arcy (2014) show that a culture of security can cause employees to comply with information security policies in the workplace [7]. Whereas according to Chang (2012), organisational commitment is another factor related to the behaviour of organisational citizen employees believe their security-conscious behaviour might cause a beneficial effect on the organisation's overall information security [8]. Organisations also need rewarding them for receiving improvements in security compliance if they want to improve compliance with information security policies [9]. This similar problem also encountered by Sommestad (2017) found a tendency to be obedient due to the habits from previous behaviour [10]. Recent Researchers agreed on the role of organisation, and the end-user is essential for information security, and several studies are examining the relationship between the role of organisations and individuals. However, limited studies investigated the relationship between organisational variables and user behaviour research on specific types of organisations such as a university. This study is to explore the factors that influence user compliance from the organisations' perspective and user habits.

The remaining part of the paper as follows: introduction, literature review, research methodology, research finding, discussion, and conclusion. This paper begins by describing a research background in the introduction section. It will then go on to section review from previous studies. After that, continue to research methodology to explain how this study conduct. The research finding explains in the following section and continues to discuss the research finding. The preceding part will discuss the limitation and conclusions

2 Literature Review

It is essential to possess a consciousness about the current issues highlighted in the literature on compliance with information security policies. Information security policies contain rules employed to create organisational IT security rules, specific problems, and system policies to address individual systems [11]. Policy documents must be obliged with precise controls and procedures for employees to implement. Otherwise, policies must be specific and detailed; hence, users can follow the guidelines [12]. Problems can arise in utilising information on security policies that become sourced from present organisations and individuals. The weakest information security chains are individuals. Therefore, it is necessary to understand how to return people in the organisation into partners for increased information security.

2.1 Organisation commitment

Measurement of organisational commitment was first introduced by Mowday (1979) to find out how employee commitment works at the organisation [13]. However, not excessively significant organisational commitment affects user behaviour. This pattern shows the impact of employee commitment on the organisation may depend on the particular behaviour that is the employee's commitment and the effect of the behaviour on organisational results [14].

The effect of an individual's prior commitment to an institution on their reaction to the perceived fairness of decisions given by the institution examined in two different field settings [15]. Information technology user behaviour in organisations can be related to the commitment to the organisation's information security, these employees believe their security-conscious behaviour affects the overall information security of the organisation. Thus, the level of organisational commitment influences the intention to follow security policies [8]. Organisational commitment focuses on staff commitment to the organisation. Organisational commitment is the most developed of all work commitment constructs [16].

2.2 Organisation culture

The organisation seeks to encourage employees to comply with information security policies when losses due to information breaches become serious. Therefore, the attention demanded such behaviour and social behaviour as an effort to constitute a substantial theoretical foundation related to security behaviour [17]. Organisations should develop policies appropriate to the culture of the organisation. Because according to Alshare (2018), organisational culture is a significant predictor for determining crime against information security policies [18]. Likewise, research conducted by Arage (2015) stated that national culture affects compliance with information security [19]. Another factor in organisations is user involvement and leadership, this potential is seen by Amankwa (2018) in his research on building a culture of compliance with information security policies in organisations using theories of organisational behaviour and organisational culture [20]. An ideal organisation

Culture prompts conscious and knowledgeable users who need to think about policies implemented by management. Organisations have reliable information security that enhances mutual trust and integration through securing their information [21].

2.3 Reward

The regulations developed must be forced on users to ensure users always obey, or users get a direct impact if they comply with policies such as getting gifts [24] getting penalties. The reward factor mentioned by the interviewee will increase employee compliance with information security policies. The reward will support the achievement of performance goals and [2] prove security compliance [9], although some researches show reward does not have a significant impact on intentions to comply with information security policies [22, 23]. This study attempted exploring the importance of rewards with compliance with information security policies.

2.4 Habit

Several researchers have examined, a habit has become one time that influences users to comply with Pahnila's information security policy [22, 24, 25]. Sommestad (2017) conducted an empirical study to develop a theory of planned behaviour used explicitly for information security compliance by adding regret and anticipated habits. [15] e results of his research found that habits did not significantly influence behavi[19]l intentions to comply with information security policies [26]. Users will adhere to IS [1] out of habit, consider them essential, and not remain a barrier to their work [27]. If people have developed good behaviour habits of information security policy compliance, compliance with their information security policies will be automatic [28]. Therefore, further research is required to use this variable with differ[14] research objects.

Based on the literature review related to user behaviour [36] pliance with information security policies, we proposed a research model described in Fig.1.

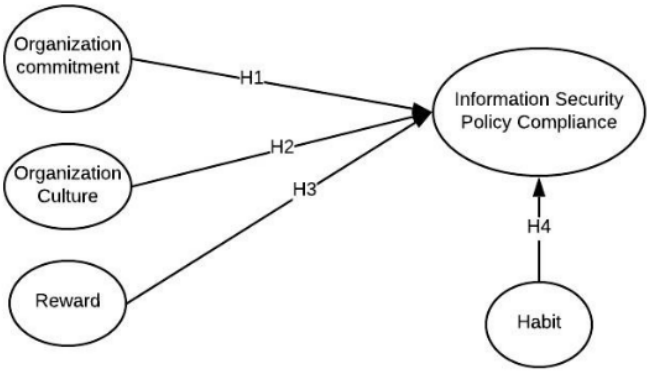

Fig. 1. Research model

This research model consisted of four variables: organisational commitment, organisation culture, reward, and habit.

The hypothesis for this study was as follows:

Hypothesis 1. organisation commitment influenced a user to comply with information security policies.

Hypothesis 2. organisation culture influenced to comply with information security policies

Hypothesis 3. reward affected users to comply with information security policy.

Hypothesis 4. habit influenced a user to comply with information security policies

3 Research Methodology

Case study for this research conducted in public universities in Indonesia. The method attempts solving the problem by conducting an online survey. Research progress describes at Fig.2 on below.

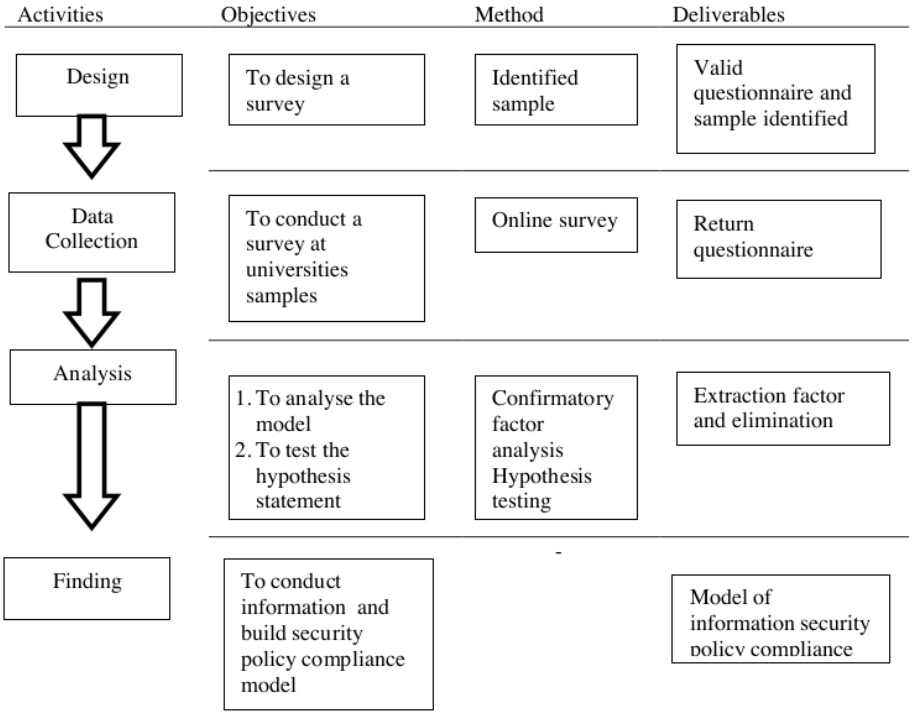

Fig. 2. Research progress

The questionnaire adapted from previous researchers: organizations' commitment [29], organization's culture [30, 31], rewards [22, 23, 32, 33] and habits [10, 22]. Invitation for the survey sends by email to university as and the questionnaire created with a google form. Online survey research can reach participants widespread as long as they have an internet connection and require anonymity [34]

The online survey conducted for two months obtained by 430 participants. Continue with data screening and encountered 412 respondents to analyse. Demography of respondents, including male (65%), women (35%), with age range 25-29 years (10%), 30-35 years (18%), 36-40 years (27%), 41-45 Years (20%), above 45 years old (25%). 80% of respondents hold Masters and PhD. 20% of respondents have work experience under two years, 3-5 years (6%), 6-10 years 98 (24%), and above ten years (65%). 9% of respondents occupy prominent positions at the university level, faculty level 15%, department level 46%, and lectures 30%. This research used Partial Least Structure (PLS) to analyse the data because this study was exploratory and used reflective variables [35].

4 Research Finding

Convergent validity used to measure model with the reflective indicator assessed based on the correlation between the component score item estimated with software PLS. Individual Reflective size was said to be high if it correlated with more than 0.70 with a measured construct. However, the early research phase of the development scale of the measurement of the loading factor in range 0.5 to 0.6 was considered adequate. In this study, it used to limit the loading *factor* of 0.50. Furthermore, discriminant validity carried out to ensure that each indicator of each latent variable differs from the other variables. The model maintained good discriminant validity if each loading value of each indicator of a latent variable possessed a more considerable loading value than other latent variables. Table 1 describes the result of convergent validity

Table 1. Convergent validity

Construct	Item code	Outer loading	Cronbach alpha	Composite reliability	The average variance extracted (AVE)
Organisation commitment (OC)	OC 1	0.909	0.949	0.958	0.739
	OC 2	0.885			
	OC 3	0.831			
	OC 4	0.816			
	OC 5	0.887			
	OC 6	0.885			
	OC 7	0.83			
	OC 8	0.83			
Organisation Culture (OL)	OL 1	0.972	0.968	0.974	0.861
	OL 2	0.969			
	OL 3	0.923			
	OL 4	0.922			
	OL 5	0.926			
	OL 6	0.85			
Reward (RW)	RW 1	0.822	0.88	0.898	0.596
	RW 2	0.839			
	RW 3	0.736			
	RW 4	0.807			
	RW 5	0.759			
	RW 6	0.654			
Habit (HA)	HA 1	0.975	0.984	0.986	0.911
	HA 2	0.966			
	HA 3	0.948			
	HA 4	0.947			
	HA 5	0.946			
	HA 6	0.947			
	HA 7	0.952			
Information security policy compliance (ISPC)	ISP1	0.888	0.848	0.899	0.692
	ISP2	0.812			
	ISP3	0.714			
	ISP4	0.9			

Table 1 explains that all outer loading values are above 0.5 so that the measurement model requirements acceptable. The loading factor value for each indicator of each latent variable did not have the most significant loading factor value compared to the loading value if it was associated with other potential variables. This value means that each latent variable had a good discriminant validity where some latent variables did not have gauges positively correlated with other constructs. Validity and reliability criteria can found from the reliability value of a construct and the value of the Average Variance Extracted (AVE) of each construct. The construct was said to have high reliability if the value was 0.70 and AVE was above 0.50. All constructs had composite reliability values above 0.70 and Cronbach's alpha above 0.60. It concluded that the construct had excellent reliability.

In PLS statistical testing, every hypothesised relationship carried out using simulations. In this case, the bootstrap method performed on the sample. Bootstrap testing also intended to minimise the problem of research data abnormalities. The estimated significance parameters provided beneficial information regarding the relationship between the research variables. Bootstrapping test results from PLS analysis could be seen in the outcome for inner weight output and testing the hypothesis of direct influence between variables based on bootstrapping presented in table 2.

Table 2. Summary of hypotheses testing

	Std. Beta	t-value	p values	Bias	Confidence interval		Decision
					2.50%	97.50%	
organization commitment -> ISP	0.042	14.297	0	-0.001	0.511	0.671	Supported
organization culture -> ISP	0.04	0.902	0.367	-0.001	-0.072	0.1	rejected
reward -> ISP	0.058	0.559	0.576	0.003	-0.165	0.086	rejected
Habit -> ISP	0.043	3.751	0	-0.002	0.084	0.247	Supported

There were four hypotheses in this study; H4, habit had a significant influence on information security policy compliance. The t-value of 3.751 was higher than the value of t-table and p-value 0.000 <0.05. The results showed that this hypothesis was acceptable and showed important habits in information security policy compliance. Second, H1 also had a very significant influence on organisational commitment. T-value 14,297 showed this variable to be the most considerable compared to other variables. However, the H2 and H3 t-value and p-value indicated no contribution and significant towards user compliance with information security policies. As a result, the organisational culture and reward variables concluded to have no relationship and influence on information security policies.

5 Discussion

The results showed that H1 and H4 were supported, while for H2 and H3, the hypothesis reject[3]. This finding showed that user habits in maintaining information security affected compliance with information[3]ecurity policies. This study stated that user habits played a role in their behaviour in complying with information security policies. Similar [30]esults found by Moody (2018), habit is a predictor that can be a predictor of user behaviour in complying with information security policies and affect intentions of precautionary action [22]. The habit of protecting information security was past behaviour, and behaviour might carry out before the information security policy implemented; therefore, it became a concern in use it to measuring compliance with information security policies. As stated by Sommestad (2017), habits can increase compliance with policies, but not as much as other behaviours [10].

Furthermore, the role of the organisation's commitment was enormous in increasing compliance with information security policies. Users would better maintain information security behaviour when they realised the organisation had responsibility for information security. Organisationa[6]commitment needed to apply to improve user security behaviour. Regulations had a direct effect on information security compliance showed [6]ganisational commitment, and then it was essential to have institutional pressure for effective information security compliance [36]. This study showed that organisational commitment variables were significant in improving user compliance behaviour towards information security policies.

The results that sur[29]ed researchers were the absence of the role of reward and organisational culture for compliance with information security policies. This study conducted with a case study at the university, so it was possible to find different results. Contrary to the research of Bulgurcu (2010), which state the rewards will impact user [8]mpliance with the policy [32]. Although previous research by Pahnila (2007), rewards do not have a significant effect on actual compliance with IS security policies [24]. Compensation used for the achievement of an objective will negatively impact [3]curity compliance [9]. Therefore, a reward given by organisations hoping to increase compliance with information security policies was considered ineffective and had no significant impact. However, reducing reward significantly affected employee attitudes towards preventing lousy behaviour in information security [37]. The users in the university exhibited different characteristics from users in other organisations. Thus, the different desired rewards affected their behaviour to adhere to the policy consistently.

6 Conclusion

This study determines factors influencing the user to comply [28]with information security [20]icy at university. The results show that organisational commitment and habit users have a significant impact on compliance with information security policy. Organisationa[8]culture and reward variables represent factors that do not receive a considerable impact on users to always comply with information security policies. Contrary to previous [14]search by Balliet (2011) says rewards have moderate to significant effects on compliance with information security policies [38.

The results provide the idea that the organisation factors have contributed to user behaviour to comply with information security policies. This finding provides significant implications for exploring how to improve user compliance with information security, especially users at universities. The results cannot claim for all universally because this research is conducted explicitly for respondents from universities. Variety respondents willing to fill out the research questionnaire come from the lecturer, and officials who have interests will affect to find another factor that is influencing the user to comply with information security policy. Further research on the selection of respondent characteristics needs to consider obtaining significant results and following the facts in the field, like involving technical employees and students as actual users of information systems at universities. This issue needs considering because information security is the responsibility of all levels of users, and all users must also comply with information security policies to fulfil the primary purpose of information security policy.

References

1. Morgan, S.: 2019 Official Annual Cybercrime Report next two decades. (2019).
2. Crossler, R.: An Extended Perspective on Individual Security Behaviors : Protection Motivation Theory and a Unified Security Practices (USP) Instrument. 45, 51–71 (2014).
3. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125 (2009). https://doi.org/10.1057/ejis.2009.6.
4. Hwang, I., Kim, D., Kim, T., Kim, S.: Why not comply with information security? An empirical approach for the causes of non-compliance. Online Inf. Rev. 41, 2–18 (2017). https://doi.org/10.1108/OIR-11-2015-0358.
5. Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Inf. Manag. 51, 69–79 (2014). https://doi.org/10.1016/j.im.2013.10.001.
6. Alotaibi, M., Furnell, S., Clarke, N.: Information Security Policies : A review of Challenges and Influencing Factors. In: The 11th International Conference for Internet Technology and Secured Transactions. pp. 352–358 (2016).https://doi.org/10.1109/ICITST.2016.7856729.
7. D'Arcy, J., Greene, G.: Security culture and the employment relationship as drivers of employees' security compliance. Inf. Manag. Comput. Secur. 22, 474–489 (2014). https://doi.org/10.1108/IMCS-08-2013-0057.
8. Chang, A.J.T., Wu, C.Y., Liu, H.W.: The effects of job satisfaction and organisation commitment on information security policy adoption and compliance. In: 2012 IEEE 6th International Conference on Management of Innovation and Technology, ICMIT 2012. pp. 442–446 (2012). https://doi.org/10.1109/ICMIT.2012.6225846.
9. Gerber, N., McDermott, R., Volkamer, M., Vogt, J.: Understanding information security compliance - Why goal setting and rewards might be a bad idea. Int. Symp. Hum. Asp. Inf. Secur. Assur. (HAISA 2016). 10., 145–155 (2016).
10. Sommestad, T., Karlzén, H., Hallberg, J.: The Theory of Planned Behavior and Information Security Policy Compliance. J. Comput. Inf. Syst. 00, 1–10 (2017). https://doi.org/10.1080/08874417.2017.1368421.
11. NIST: Glossary of Key Information Security Terms [NISTIR 7298 Rev 2]. (2013). https://doi.org/10.1016/0735-6757(85)90039-7.

12. Wright, C.: Assessing Security Awareness and Knowledge of Policy. In: The IT Regulatory and Standards Compliance Handbook. pp. 161–194 (2008).
13. Mowday, R.T.: Reflections on the study and relevance of organisational commitment. Hum. Resour. Manag. Rev. 8, 387–401 (1998). https://doi.org/10.1016/S1053-4822(99)00006-6.
14. Angle, H.L., Perry, J.L.: An Empirical Assess- ment of Organizational Commitment and Organizational Effective- ness. Adm. Sci. Q. 26, 1–14 (1981).
15. Brockner, J., Tyler, T.R., Cooper-Schneider, R.: The Influence of Prior Commitment to an Institution on Reactions to Perceived Unfairness: The Higher They Are, The Harder They Fall. Adm. Sci. Q. 37, 241 (1992). https://doi.org/10.2307/2393223.
16. Amin, M., Barati, O., Ghoroghchian, M.: Role of Organizational Climate in Organizational Commitment : The Case of Teaching Hospitals. Osong Public Heal. Res. Perspect. 7, 96–100 (2016). https://doi.org/10.1016/j.phrp.2015.11.009.
17. Han, J.Y., Kim, Y.J., Kim, H.: An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. Comput. Secur. 66, 52–65 (2017). https://doi.org/10.1016/j.cose.2016.12.016.
18. Alshare, K.A., Lane, P.L., Lane, M.R.: Information security policy compliance: a higher education case study. Inf. Comput. Secur. 26, 91–108 (2018). https://doi.org/10.1108/ICS-09-2016-0073.
19. Arage, T., Belanger, F., Beshah, T.: Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies. In: AMCIS 2015 Proceedings. pp. 1–7 (2015).
20. Amankwa, E., Loock, M., Kritzinger, E.: Establishing information security policy compliance culture in organisations. Inf. Comput. Secur. 26, 420–436 (2018). https://doi.org/10.1108/ICS-09-2017-0063.
21. da Veiga, A., Astakhova, L. V., Botha, A., Herselman, M.: Defining organisational information security culture – Perspectives from academia and industry. Comput. Secur. 101713 (2020). https://doi.org/10.1016/j.cose.2020.101713.
22. Moody, G.D., Siponen, M., Pahnila, S.: Toward a Unified Model of Information Security Policy Compliance. MIS Q. 42, 285–311 (2018). https://doi.org/10.25300/MISQ/2018/13853.
23. Siponen, M., Adam Mahmood, M., Pahnila, S.: Employees' adherence to information security policies: An exploratory field study. Inf. Manag. 51, 217–224 (2014). https://doi.org/10.1016/j.im.2013.08.006.
24. Pahnila, S., Siponen, M., Mahmood, A.: Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. Pacis 2007 Proc. 438–439 (2007). https://doi.org/10.1007/978-0-387-72367-9_12.
25. Siponen, M., Pahnila, S., Mahmood, m. adam: Compliance with Information Security Policies: An Empirical Investigation. IEEE Comput. Soc. (2010).
26. Sommestad, T., Karlzén, H., Hallberg, J.: The Theory of Planned Behavior and Information Security Policy Compliance The Theory of Planned Behavior and Information Security Policy Compliance. J. Comput. Inf. Syst. 00, 1–10 (2017). https://doi.org/10.1080/08874417.2017.1368421.
27. Topa, I., Karyda, M.: From theory to practice: guidelines for enhancing information security management. Inf. Comput. Secur. 27, 326–342 (2019). https://doi.org/10.1108/ICS-09-2018-0108.
28. Hong, Y., Furnell, S.: Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. J. Comput. Inf. Syst. 00, 1–10 (2019). https://doi.org/10.1080/08874417.2019.1683781.

29. Mowday, R.T., Steers, R.M., Porter, L.W.: The Masurement of Organizational Commitment : A Progress Report. J. Vocat. Behav. 14, 224–247 (1979).
30. Hogail, A. Al: Cultivating and assessing an organisational information security culture; an empirical study. Int. J. Secur. its Appl. 9, 163–178 (2015). https://doi.org/10.14257/ijsia.2015.9.7.15.
31. Martins, A., Eloff, J.: Information Security Culture. 191–201 (2002). https://doi.org/10.1007/978-0-387-35586-3_15.
32. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Q. 34, 523–548 (2010). https://doi.org/10.1093/bja/aeq366.
33. Beckers, K., Cote, I., Fenz, S., Hatebur, D., Heisel, M.: A Structured Comparison of Security Standards. In: Engineering Secure Future Internet Services and Systems. pp. 1–34. Springer International Publishing, Switzerland (2014). https://doi.org/10.1007/978-3-319-07452-8.
34. Sue, V., Ritter, L.: Conducting Online Surveys. (2015). https://doi.org/10.4135/9781506335186.
35. Ringle, C.M., Sarstedt, M., Straub, D.: A critical look at the use of PLS-SEM in MIS Quarterly. MIS Q. 36, iii–xiv (2012). https://doi.org/10.3200/JOEB.79.4.213-216.
36. Alkalbani, A., Deng, H., Zhang, X.J.: Investigating the Impact of Institutional Pressures on Information Security Compliance in Organisations. Australas. Conf. Inf. Syst. 1–12(2016).
37. Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M., Sookhak, M.: Deterrence and prevention-based model to mitigate information security insider threats in organisations. Futur. Gener. Comput. Syst. 97, 587–597 (2019). https://doi.org/10.1016/j.future.2019.03.024.
38. Balliet, D., Mulder, L.B., M Van Lange, P.A., Lange, V., M, P.A.: Reward, Punishment, and Cooperation: A Meta-Analysis Citation. Psychol. Bull. 137, 594–615 (2011). https://doi.org/10.1037/a0023489.

Affecting Factors in Information Security Policy Compliance: Combine Organisational Factors and User Habits

ORIGINALITY REPORT

16%	9%	13%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.tandfonline.com Internet Source	1%
2	Mikko Siponen. "Employees' Adherence to Information Security Policies: An Empirical Study", IFIP International Federation for Information Processing, 2007 Publication	1%
3	Siponen, Mikko, Seppo Pahnila, and M. Adam Mahmood. "Compliance with Information Security Policies: An Empirical Investigation", Computer, 2010. Publication	1%
4	www.arjonline.org Internet Source	1%
5	Submitted to Universitas 17 Agustus 1945 Surabaya Student Paper	1%
6	aisel.aisnet.org Internet Source	1%

7	www.researchgate.net Internet Source	1%
8	docplayer.net Internet Source	1%
9	Submitted to Anoka Technical College Student Paper	1%
10	Mohammad Amin Bahrami, Omid Barati, Malake-sadat Ghoroghchian, Razieh Montazer-alfaraj, Mohammad Ranjbar Ezzatabadi. "Role of Organizational Climate in Organizational Commitment: The Case of Teaching Hospitals", Osong Public Health and Research Perspectives, 2016 Publication	1%
11	Sadaf Hina, Dhanapal Durai Dominic. "Need for information security policies compliance: A perspective in Higher Education Institutions", 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), 2017 Publication	<1%
12	fr.m.wikipedia.org Internet Source	<1%
13	David Sikolia, Douglas Twitchell, Glen Sagers. "Protection Motivation and Deterrence: Evidence from a Fortune 100 Company", AIS	<1%

Transactions on Replication Research, 2018
Publication

14	Liisa Myyry, Mikko Siponen, Seppo Pahnila, Tero Vartiainen, Anthony Vance. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", European Journal of Information Systems, 2017 Publication	<1%
15	Tejaswini Herath, H Raghav Rao. "Protection motivation and deterrence: a framework for security policy compliance in organisations", European Journal of Information Systems, 2017 Publication	<1%
16	morro-bay.ca.us Internet Source	<1%
17	"Advances in Production Management Systems. Towards Smart and Digital Manufacturing", Springer Science and Business Media LLC, 2020 Publication	<1%
18	hdl.handle.net Internet Source	<1%
19	Ioanna Topa, Maria Karyda. "From theory to practice: guidelines for enhancing information security management", Information & Computer Security, 2019	<1%

Publication

20	Michael Foth. "Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence", European Journal of Information Systems, 2017 Publication	<1%
21	Yousef Mohammad Iriqat, Abd Rahman Ahlan, Nurul Nuha Abdul Molok. "Information Security Policy Perceived Compliance Among Staff in Palestine universities: An Empirical Pilot study", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019 Publication	<1%
22	link.springer.com Internet Source	<1%
23	www.gbmrjournal.com Internet Source	<1%
24	Hu, Qing, Tamara Dinev, Paul Hart, and Donna Cooke. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture* : Managing Employee Compliance with Information Security Policies", Decision Sciences, 2012. Publication	<1%

25	Choi, Myeonggil. "Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing", Sustainability, 2016. Publication	<1%
26	A. J. Burns, Tom L. Roberts, Clay Posey, Rebecca J. Bennett, James F. Courtney. "Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts*", Decision Sciences, 2017 Publication	<1%
27	creativecommons.org Internet Source	<1%
28	koreascience.or.kr Internet Source	<1%
29	uir.unisa.ac.za Internet Source	<1%
30	Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. "Information security conscious care behaviour formation in organizations", Computers & Security, 2015. Publication	<1%
31	Elham Rostami, Fredrik Karlsson, Shang Gao.	

	"Requirements for computerized tools to design information security policies", Computers & Security, 2020 Publication	<1%
32	www.usenix.org Internet Source	<1%
33	Surayahani Hasnul Bhaharin, Umi Asma' Mokhtar, Rossilawati Sulaiman, Maryati Mohd Yusof. "Issues and Trends in Information Security Policy Compliance", 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), 2019 Publication	<1%
34	Ahmad Al-Omari, Omar El-Gayar, Amit Deokar. "Security Policy Compliance: User Acceptance Perspective", 2012 45th Hawaii International Conference on System Sciences, 2012 Publication	<1%
35	Kwame Simpe Ofori, Hod Anyigba, George Oppong Appiagyei Ampong, Osaretin Kayode Omoregie, Makafui Nyamadi, Eli Fianu. "chapter 10 Factors Influencing Information Security Policy Compliance Behavior", IGI Global, 2020 Publication	<1%
36	"Software Engineering Perspectives in Intelligent Systems", Springer Science and Business	<1%

Media LLC, 2020
Publication

37	Eric Amankwa, Marianne Loock, Elmarie Kritzinger. "Chapter 51 A Composite Framework to Promote Information Security Policy Compliance in Organizations", Springer Science and Business Media LLC, 2020 Publication	<1%
38	jyx.jyu.fi Internet Source	<1%
39	Adéle da Veiga, Liudmila V. Astakhova, Adéle Botha, Marlien Herselman. "Defining organisational information security culture—Perspectives from academia and industry", Computers & Security, 2020 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		